IN THE CLAIMS

Please find below a listing of all of the pending claims. The status of each claim is set forth in parentheses. This listing will replace all prior versions, and listings, of claims in the present application.

1. (Currently Amended) A method of controlling processing of data in a computer apparatus, wherein the data comprises a plurality of usage rules for a plurality of data items stored by said computer apparatus, and comprising:

applying, by a computer, different individualised usage rules to each of the data items based on a measurement of integrity of a computing entity to which the data items are to be made available, wherein the measurement of integrity is a measure of whether the computing entity includes a trusted platform providing controlled and audited levels of privacy for the data items and said data items ~~being~~ are logically grouped together as a set of data items, and

instantiating the set of data items at the computing entity depending upon the integrity of the computing entity and the usage rule applicable to each data item in said set.

2. (Original) A method as claimed in claim 1, in which at least some of the usage rules comprise masking instructions for masking the associated data items.

3. (Original) A method as claimed in claim 2, in which a data item is masked from a set of data by encrypting it.

4. (Original) A method as claimed in claim 3, in which a data item is encrypted with an associated encryption key, said encryption key being different for different ones of the data items.

5. (Original) A method as claimed in claim 1, in which the usage rules define security rules for the associated data item.

6. (Original) A method as claimed in claim 1, in which the data may be transferred between a plurality of computing entities and the instantiation of the data at each computing entity depends on the capabilities of that entity.

7. (Original) A method as claimed in claim 6, in which a computing entity is a computing platform.

8. (Original) A method as claimed in claim 6, in which the computing entity is a software process.

9. (Original) A method as claimed in claim 1, in which a computing entity can reliably and irrevocably deny future access to selected data items.

10. (Original) A method as claimed in claim 9, in which means for accessing the data is stored within a protected memory.

11. (Original) A method as claimed in claim 10, in which the protected memory is within a trusted computing module.

12. (Original) A method as claimed in claim 1, in which computing entities negotiate with one another concerning the use of the data before the data is made available.

13. (Original) A method as claimed claim 1, in which the data has constraints defining conditions for use of the data.

14. (Original) A method as claimed in claim 13, in which the constraints define at least one item selected from:

a. the purpose for which the data can be used

b. the geographical area in which the data may be manifested

c. the temporal domain in which the data may be manifested

d. the computing platforms that may manipulate the data.

15. (Original) A method as claimed in claim 1 in which the data further includes test data.

16. (Original) A method as claimed in claim 15, in which the structure of test data is comparable to the structure of real data contained by the data items.

17. (Original) A method as claimed in claim 16, in which the results of operations performed on the test data are examined in order to make a decision on whether to release the real data to a node that operated on the test data.

18. (Original) A method as claimed in claim 1, in which a node requesting access to the data supplies hostage material to the node issuing the data prior to the issuance of the data.

19. (Original) A method as claimed in claim 18, in which a third party hostage release authority is contacted to activate the hostage material.

20. (Original) A method as claimed in claim 1 in which a node finding itself in possession of data whose history or content do not meet predetermined requirements, formats the data and places it in a repository.

21. (Original) A method as claimed in claim 20, in which the data placed in the repository is in an encrypted form.

22. (Original) A method as claimed in claim 21, in which the data is encrypted using a public key included in the data.

23. (Previously Presented) A method as claimed in claim 21, in which the data in the repository is associated with an identification means to enable the owner of the data to identify it.

24. (Original) A method as claimed in claim 1, in which a node wishing to present the data for retrieval places the data in a repository.

25. (Original) A method as claimed in claim 24, in which the data is placed in the repository in encrypted form.

26. (Original) A method as claimed in claim 25, in which the data is encrypted using a public key included in the data.

27. (Original) A method as claimed in claim 26, in which the data in the repository is associated with identification means to enable the owner of the data to identify it.

28. (Original) A method as claimed in claim 1, in which constraints associated with the data determine whether the data will process on anything other than a trusted computing platform.

29. (Original) A method as claimed in claim 28, in which constraints associated with the data determine whether the data and/or results from processing the data are inhibited from viewing by a computing platform owner or administrator.

30. (Original) A method as claimed in claim 1 in which the security contracts are stored separately from the data.

31. (Original) A method as claimed in claim 1 in which mask or decryption keys are stored separately from the data.

32. (Original) A method as claimed in claim 1 in which a computing entity that receives data signs the data with a signature key belonging to that entity.

33. (Currently Amended) A method of controlling processing of data, wherein the data comprises a plurality of rules associated with a plurality of data items, the method comprising:

applying, by a computer, different rules to the data items ~~a set of logically related data items~~, each data item in the set having a rule of the rules associated therewith, said rules acting to individually define at least one of usage and~~/or~~ security to be observed when processing each of the data items in the set of data items[[,]]; and

~~in which~~ forwarding ~~of~~ the ~~set of~~ data items ~~is performed~~ in accordance with mask means provided in association with the rules.

34. (Original) A method as claimed in claim 33, in which the mask comprises at least one of a symmetric encryption string, symmetric encryption key, and an asymmetric encryption key.

35. (Original) A method as claimed in claim 33, in which the rules associated with the data items are adhered to in preference to data handling rules associated with a computing entity processing the data.

36. (Original) A method as claimed in claim 33, in which at least some of the rules comprise masking instructions for masking the associated data items.

37. (Original) A method as claimed in claim 36, in which a data item is masked from a set of data by encrypting it.

38. (Original) A method as claimed in claim 37, in which a data item is encrypted with an associated encryption key, said encryption key being different for different ones of the data items.

39. (Original) A method as claimed in claim 33 in which the data may be transferred between computing entities and the instantiation of the data at each computing entity depends on the capabilities of the entity.

40. (Previously Presented) A method as claimed in claim 33, in which the rules define at least one item selected from:

a. the purpose for which the data can be used

b. the geographical area in which the data may be manifested

c. the temporal domain in which the data may be manifested

d. the computing platforms that may manipulate the data.

41. (Original) A method as claimed in claim 33 in which the data further includes test data, the test data is comparable to the structure of real data contained by the data items, and in

which the results of operations performed on the test data are examined in order to make a decision on whether to release the real data to node that operated on the test data.

42. (Original) A method as claimed in claim 33, in which a computing entity finding itself in possession of data whose history or content do not meet predetermined requirements, or wishing to make data available because it has performed some processing in at least partially masked form, formats the data places it in a repository.

43. (Currently Amended) A computer program stored on a non-transitory computer readable media for instructing a programmable computer to implement a method of controlling the processing of data, wherein the data comprises a plurality of usage rules for a plurality of data items, the method implemented by the computer executing the computer program comprising:

~~programmable computer being programmed to~~ applying different individualised usage rules to each of the data items based on a measurement of integrity of a computing entity to which the data items are to be made available, wherein the measurement of integrity is a measure of whether the computing entity includes a trusted platform providing controlled and audited levels of privacy for the data items; and

~~the computer program~~ permitting instantiation of the data items at the computing entity only if the integrity of the computing entity complies with the individualised usage rules associated with said data items.

Claims 44-49. (Cancelled)

50. (Currently Amended) A computer apparatus for controlling processing of data, wherein the data comprises a plurality of usage rules for a plurality of data items stored by said computer apparatus, said computer apparatus controlling instantiation of the data at a computing entity, said computer apparatus including:

programming, executed by the computer apparatus, for applying different individualised usage rules to each of the data items based on a measurement of integrity of the computing entity to which the data items are to be made available, wherein the measurement of integrity is a measure of whether the computing entity includes a trusted platform providing controlled and audited levels of privacy for the data items and said data items being logically grouped together as a set of data items, and

programming, executed by the computer apparatus, for individually instantiating data items in the set of data items at the computing entity as a function of the integrity of the computing entity and the usage rule applicable to each data item in said set.